

In the Claims:

Please amend the Claims as follows:

1. (Currently Amended) A hybrid digital watermarking system for video authentication, the system comprising:

an authenticated acquisition subsystem for digitally watermarking video data; and

a video management subsystem in signal communication with the authenticated acquisition subsystem for verifying the digitally watermarked video data; and

signature means for applying a control signature to the video data,

wherein the signature means embeds signature bits into data blocks in accordance with a pseudo-random sequence that introduces a dependency among the blocks,

wherein the pseudo-random sequence is generated from a data-dependent seed extracted from at least one frame,

wherein the seed is responsive to at least one DC coefficient, and

wherein the at least one DC coefficient is coarsely quantized prior to seed generation.

2. (Original) A system as defined in Claim 1 wherein the video management subsystem is in intermittent signal communication with the authenticated acquisition subsystem.

3. (Original) A system as defined in Claim 1, the authenticated acquisition subsystem comprising a video imaging device for acquiring original video data.

4. (Original) A system as defined in Claim 1, the authenticated acquisition subsystem comprising a watermarking device for applying each of an identity signature and a control signature to the video data.

5. (Original) A system as defined in Claim 4 wherein the control signature comprises fragile control bits and robust control bits.

6. (Original) A system as defined in Claim 4 wherein the identity signature and the control signature are applied to the video data concurrent with real-time acquisition of the video data.

7. (Original) A system as defined in Claim 4 wherein the identity signature and the control signature are embodied in a single hybrid digital watermark.

8. (Original) A system as defined in Claim 7 wherein the single hybrid digital watermark achieves progressively varying robustness in a single watermark by means of at least one of error-correcting signature coding and rate-distortion guided bit embedding.

9. (Original) A system as defined in Claim 1, the video management subsystem comprising a verification device for verifying a control signature and an identity signature.

10. (Original) A system as defined in Claim 9 wherein the identity signature and the control signature are extracted from a single digital watermark.

11. (Original) A system as defined in Claim 1, the video management subsystem comprising a watermark verifying playback device for verifying a control signature and an identity signature and displaying verified video data.

12. (Original) A system as defined in Claim 11 wherein the watermark verifying playback device alerts a user to the presence of altered video content.

13. (Currently Amended) A method of hybrid digital watermarking for video authentication, the method comprising:

digitally watermarking video data; and

verifying the digitally watermarked video data;
applying a control signature to the video data;
embedding bits of the control signature into data blocks in accordance
with a pseudo-random sequence that introduces a dependency among the
blocks;
extracting a data-dependent seed from at least one frame, wherein the
seed is responsive to at least one DC coefficient;
generating the pseudo-random sequence from the extracted seed; and
applying a coarse quantizer to the at least one DC coefficient prior to seed
generation.

14. (Original) A method as defined in Claim 13, further comprising
intermittently transmitting the digitally watermarked video data prior to
verification.

15. (Original) A method as defined in Claim 13, further comprising
compressing the digitally watermarked video data prior to verification.

16. (Original) A method as defined in Claim 15 wherein compressing
comprises Moving Pictures Expert Group ("MPEG") encoding the digitally
watermarked video data prior to verification.

17. (Original) A method as defined in Claim 16 wherein compressing comprises MPEG-2 encoding the digitally watermarked video data prior to verification.

18. (Original) A method as defined in Claim 16 wherein compressing comprises MPEG-4 encoding the digitally watermarked video data prior to verification.

19. (Original) A method as defined in Claim 13, further comprising acquiring original video data.

20. (Original) A method as defined in Claim 19 wherein the acquired original video data is in Digital Video ("DV") format.

21. (Original) A method as defined in Claim 13, further comprising applying each of an identity signature and a control signature to the video data.

22. (Original) A method as defined in Claim 21 wherein the control signature comprises fragile control bits and robust control bits.

23. (Original) A method as defined in Claim 21, further comprising embedding bits of the control signature into data blocks in accordance with a pseudo-random sequence that introduces a dependency among the blocks.

24. (Original) A method as defined in Claim 23, further comprising:
extracting a data-dependent seed from at least one frame; and
generating the pseudo-random sequence from the extracted seed.

25. (Original) A method as defined in Claim 24, further comprising generating the seed for the pseudo-random sequence in accordance with a hash function.

26. (Original) A method as defined in Claim 25 wherein the seed is responsive to at least one DC coefficient.

27. (Original) A method as defined in Claim 26, further comprising applying a coarse quantizer to the at least one DC coefficient prior to seed generation.

28. (Original) A method as defined in Claim 27 wherein the at least one DC coefficient is selected from a plurality of data blocks having a DC coefficient value close to a quantization level of the coarse quantizer.

29. (Original) A method as defined in Claim 21 wherein the identity signature and the control signature are applied to the video data concurrent with real-time acquisition of the video data.

30. (Original) A method as defined in Claim 21 wherein the identity signature and the control signature are embodied in a single hybrid digital watermark.

31. (Original) A method as defined in Claim 30, further comprising at least one of:

coding error-correcting signatures in the single hybrid digital watermark;

and

embedding rate-distortion guided bits in the single hybrid digital watermark to achieve progressively varying robustness.

32. (Original) A method as defined in Claim 13, further comprising verifying a control signature and an identity signature.

33. (Original) A method as defined in Claim 32 wherein the identity signature and the control signature are extracted from a single digital watermark.

34. (Original) A method as defined in Claim 13, further comprising:
verifying a control signature and an identity signature; and
displaying verified video data.

35. (Original) A method as defined in Claim 34, further comprising
producing an alert responsive to the presence of altered video content.

36. (Original) A method as defined in Claim 15, further comprising
detecting tampering in coordination with knowledge specific to the compression
domain.

37. (Original) A method as defined in Claim 36 wherein the compression
domain comprises DCT encoded data.

38. (Original) A method as defined in Claim 36 wherein the knowledge
specific to the compression domain comprises at least one of spatial and
temporal dependencies.

39. (Original) A method as defined in Claim 36, further comprising:
assigning a likelihood value for possible tampering to each error block
based its number of neighbors; and

temporally integrating the likelihood values to compute a score map indicative of potentially tampered regions.

40. (Withdrawn) A digital video data file encoded with signal data comprising a plurality of block transform coefficients, the coefficients collectively indicative of an original video data sequence with an added hybrid watermark, the watermark comprising each of an identity signature and a control signature.

41. (Withdrawn) A digital video data file as defined in Claim 40 wherein the control signature comprises fragile control bits and robust control bits.

42. (Withdrawn) A digital video data file as defined in Claim 40, the data file achieving progressively varying robustness in a single watermark by means of at least one of error-correcting signature coding and rate-distortion guided bit embedding.

43. (Withdrawn) A digital video data file as defined in Claim 42, the data file being embodied in a Digital Video Disk ("DVD").

44. (Original) A hybrid digital watermarking system for video authentication as defined in Claim 1, the system further comprising watermark means for digitally watermarking the video data.

45. (Original) A system as defined in Claim 44, further comprising verification means in signal communication with the watermark means for verifying the digitally watermarked video data.

46. (Original) A system as defined in Claim 45, further comprising transmission means for intermittently transmitting the digitally watermarked video data prior to verification.

47. (Original) A system as defined in Claim 45, further comprising compression means for compressing the digitally watermarked video data prior to verification.

48. (Original) A system as defined in Claim 47 wherein the compression means comprises encoding means for Moving Pictures Expert Group ("MPEG") encoding the digitally watermarked video data prior to verification.

49. (Original) A system as defined in Claim 48 wherein the encoding means comprises MPEG-2 encoder means for encoding the digitally watermarked video data prior to verification.

50. (Original) A system as defined in Claim 48 wherein the encoding means comprises MPEG-4 encoder means for encoding the digitally watermarked video data prior to verification.

51. (Original) A system as defined in Claim 45, further comprising imaging means for acquiring original video data.

52. (Original) A system as defined in Claim 51 wherein the imaging means acquires original video data in Digital Video ("DV") format.

53. (Original) A system as defined in Claim 45, further comprising signature means for applying each of an identity signature and a control signature to the video data.

54. (Original) A system as defined in Claim 53 wherein the signature means applies the identity signature and the control signature to the video data concurrent with real-time acquisition of the video data.

55. (Original) A system as defined in Claim 53 wherein the signature means is in signal communication with the watermark means for combining the identity signature and the control signature in a single hybrid digital watermark.

56. (Original) A system as defined in Claim 55, further comprising at least one of:

coding means for coding error-correcting signatures in the single hybrid digital watermark; and

embedding means in signal communication with the encoding means for embedding rate-distortion guided bits in the single hybrid digital watermark to achieve progressively varying robustness.

57. (Original) A system as defined in Claim 55, further comprising verification means for verifying a control signature and an identity signature.

58. (Original) A system as defined in Claim 57 wherein the verification means extracts the identity signature and the control signature from a single digital watermark.

59. (Original) A system as defined in Claim 55, further comprising:

signature verification means for verifying at least one of a control signature and an identity signature; and

display means in signal communication with the signature verification means for displaying verified video data.

60. (Original) A system as defined in Claim 59, further comprising alert means for producing an alert responsive to the presence of altered video content.

61. (Original) A system as defined in Claim 47, the verification means comprising tamper detection means responsive to knowledge specific to the compression domain.

62. (Original) A system as defined in Claim 61 wherein the compression domain comprises DCT encoded data.

63. (Original) A system as defined in Claim 61 wherein the knowledge specific to the compression domain comprises at least one of spatial and temporal dependencies.

64. (Original) A system as defined in Claim 61, further comprising:
likelihood means for assigning a likelihood value for possible tampering to each error block based its number of neighbors; and
temporal integration means for temporally integrating the likelihood values to compute a score map indicative of potentially tampered regions.

65. (Original) A system as defined in Claim 53 wherein the signature means embeds signature bits into data blocks in accordance with a pseudo-random sequence that introduces a dependency among the blocks.

66. (Original) A system as defined in Claim 65 wherein the pseudo-random sequence is generated from a data-dependent seed extracted from at least one frame.

67. (Original) A system as defined in Claim 66 wherein the seed for generating the pseudo-random sequence is itself generated using a hash function.

68. (Original) A system as defined in Claim 67 wherein the seed is responsive to at least one DC coefficient.

69. (Original) A system as defined in Claim 68 wherein the at least one DC coefficient is coarsely quantized prior to seed generation.